激励方法-selfish攻击
同时关注于自私问题和隐私问题（机会网络中的相遇事件会揭露节点的位置信息，甚至可以用来推断节点的身份信息），
采用时间相关的指数函数和线性函数分别建模消息价值和转发花费，利用TA维护每个节点的真实/虚假ID并进行目的节点
付费和中继节点奖励，从而在激励节点参与合作的同时保护节点隐私

IPAD: An Incentive and Privacy-Aware Data Dissemination Scheme in Opportunistic Networks

Rongxing Lu[†], Xiaodong Lin[‡], Zhiguo Shi[†,§], Bin Cao[†,¶], and Xuemin (Sherman) Shen[†]
[†]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
[‡]Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Ontario, Canada
[§]Zhejiang University, Hangzhou 310027, China; [¶]CERC, Harbin Institute of Technology, Shenzhen, 518055, China
Email: {rxlu, xshen}@bbcr.uwaterloo.ca; xiaodong.lin@uoit.ca; shizg@zju.edu.cn; caobin@hitwh.edu.cn

***Abstract*—Opportunistic network (OPPNET) is characterized by the intermittent connectivity among mobile nodes from their unpredictable mobility. Although it is promising, there still exist many security and privacy challenges. In this paper, we present an incentive and privacy-aware data dissemination (IPAD) scheme for OPPNETs, not only to exploit how to protect mobile node's identity privacy, location privacy and social profile privacy, but also to provide a secure incentive for privacy-aware data dissemination. Through extensive incentive analysis, we show that only if a source provides a secure incentive strategy, can a data packet be efficiently disseminated in OPPNETs.**

***Keywords* – Opportunistic network; Data dissemination; Incentive; Privacy-Aware**

I. Introduction

Opportunistic Networks (OPPNETs) [1], such as delay tolerant networks [2], vehicular communication networks [3], and ubiquitous mobile social networks [4], have received considerable research attention in recent years. As an interesting evolution of MANETs, OPPNETs are more pervasive and distinguishably characterized by non-exist end-to-end connection, but intermittent connectivity among mobile nodes during their opportunistic contacts [1]. However, due to the extremely dynamic and unstable network topology, the packet propagation in OPPNETs usually follows a "store-carry-and-forward" manner, and the packets can only be opportunistically relayed to their destinations with high transmission delay and low delivery ratio. In order to reduce the transmission delay and increase the delivery ratio, extensive research efforts have recently been put into OPPNET routing and dissemination, and a variety of efficient routing and dissemination protocols [5]–[7], which either rely on network and mobility characteristics [5], [6] or utilize pre-existing social network information [7], have been proposed for OPPNETs.

Despite the significant progress, selfish and privacy issues, two crucial human factors in OPPNETs, have not been fully exploited in the above protocols, which may make them impractical in real-world OPPNET scenarios. A common hypothesis made in the above protocols is that all nodes are cooperative, i.e., each node is willing to relay packets for others voluntarily. However, in order to conserve energy, storage and computing resources, some nodes could behave selfishly and will not participate in relaying, which thus violates the hypothesis and makes these well-designed protocols inefficient. To this end, it is imperative to provide some incentive strategies to stimulate selfish nodes to nodal cooperation in OPPNETs [7], [8]. In addition to the selfish issue, privacy issue is also challenging in OPPNETs [9]. If the privacy of node is not well protected, nodes will be still reluctant to participate in nodal cooperation. For example, some protocols study node mobility to improve the network performance, but the node mobility will disclose node's location privacy [10]; other protocols use the pre-existing social network information to accelerate the packet delivery, however the social network information will also depressively release node' identity privacy and social profile privacy [7]. Since huge security and privacy risks are heavily associated with OPPNETs, how to deal with privacy challenges is crucial for the success of OPPNETs [10], [11].

Although both selfish and privacy issues have been identified as two crucial human factors for the wide acceptance of OPPNETs, many recent research works [7]–[11] tend to separately study them in OPPNETs. The reason is that, if the selfish and privacy issues are addressed at the same time in OPPNETs, the problem would become more challenging. For example, some privacy enhanced techniques [12] enable a node to hide its identity and location information, but they could make some incentive strategies, especially the reputation-based incentive strategies, hard to implement in OPPNETs, since a node is no longer identified, and its activities cannot be linked. Therefore, how to simultaneously address selfish and privacy issues becomes particularly challenging in OPPNETs.

In this paper, aiming at addressing the above challenge, we propose a new credit-based Incentive and Privacy-Aware data Dissemination scheme, called IPAD, for OPPNETs. In IPAD, each node holds a family of unlinkable pseudo-IDs and periodically change its current pseudo-ID for privacy preservation. When a source node wants to disseminate a time-valuable data to a group of social friends, it also attaches an incentive on the data packet. Then, selfish nodes can be stimulated to participate in relaying to improve the dissemination ratio and reduce the average delay in OPPNETs.

The remainder of this paper is organized as follows. In Section II, we formalize the network model, incentive model, security model and identify our design goal. Then, we present

This work is supported by ORF-RE, Ontario, Canada, and National Science Foundation of China (No. 61171149).

WoWMoM 似乎 经常发表一些OppNet
路由算法

978-1-4673-5946-7/13/$31.00 ©2013 IEEE

the IPAD scheme in Section III, followed by the incentive analysis in Section IV. Finally, we draw our conclusions in Section V.

II. Models and Design Goal

In this section, we formalize the network model, incentive model, security model and identify our design goal.

A. Network Model

In our network model, we consider a homogenous OPPNET which is composed of a set of n mobile nodes $\mathcal{N} = \{N_0, N_1, \cdots, N_{n-1}\}$ with the same transmission radius tr moving in a terrain area, as shown in Fig. 1. All mobile nodes follow the same random-based mobility model, e.g., random waypoint, with the same velocity v. According to [13], the pairwise user inter-contact time between any two nodes under this model can be assumed to be exponentially distributed, and the contacts between them form a Possion process with the contact rate λ.

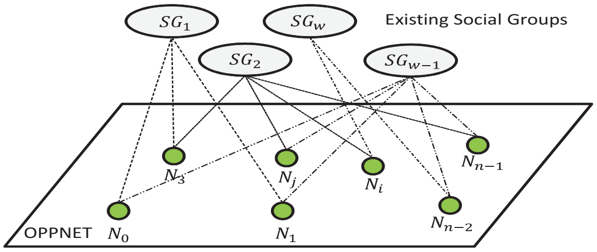


Fig. 1. OPPNET network model under consideration

In addition to the physical OPPNET, we also consider there exist some predefined virtual social groups $\mathcal{SG} = \{SG_1, SG_2, \cdots, SG_w\}$, as shown in Fig. 1, each $SG_j \in \mathcal{SG}$ has its specific theme. If a node $N_i \in \mathcal{N}$ is a member of SG_j, it shares a group key K_j of SG_j, which will be used by N_i to access all sessions in SG_j. Note that, N_i could belong to multiple virtual social groups, and these social affiliations are sensitive to N_i, and should be kept securely in N_i's social profile. In the OPPNET under consideration, a source $S \in SG_j$ can distribute a data packet M to other members in SG_j via the movement of mobile nodes $\mathcal{N} = \{N_0, N_1, \cdots, N_{n-1}\}$ with proper data dissemination algorithms. Through a "store-carry-and-forward" pattern, the data packet can be finally relayed to the destinations $SG_j/\{S\}$.

B. Incentive Model

Each mobile node $N_i \in \mathcal{N}$ is rational, and it always tries to maximize its utility. In our incentive model, mobile nodes $\mathcal{N} = \{N_0, N_1, \cdots, N_{n-1}\}$ can be categorized into two types: the source S, and the other nodes $\mathcal{N}/\{S\}$. Assume that the data packet M with Time-to-Live (TTL) setting has a time value, then the value of M can be represented as a time-dependent decreasing function $\mathsf{V}(M, t_i)$. For example, if one destination $N_i \in SG_j/\{S\}$ receives the data packet M at time $t_i \geq 0$, the value $\mathsf{V}(M, t_i)$ to N_i is defined as

pkt早一点被收到，消息价值就比较高

$$\mathsf{V}(M, t_i) = \begin{cases} \mathbf{v}_m \cdot e^{-\mathbf{k}_m(t_i - TTL)}, & \text{if } 0 \leq t_i \leq TTL \\ 0, & \text{if } t_i > TTL \end{cases} \tag{1}$$

where $\mathbf{v}_m$ is the base value of M, and $\mathbf{k}_m$ is the rate at which the value would decrease. Correspondingly, N_i will pay $\mathsf{V}(M, t_i)$ to the source S for receiving M. Assume all destinations $SG_j/\{S\}$ receive M before TTL, the total payoff for the source S would be $\mathsf{P}_M = \sum_{N_i \in SG_j/\{S\}} \mathsf{V}(M, t_i) = \mathbf{v}_m \cdot \sum_{N_i \in SG_j/\{S\}} e^{-\mathbf{k}_m(t_i - TTL)}$. Therefore, in order to maximize the payoff P_M, the source S needs more relay nodes to disseminate M to more destinations as quickly as possible.

中继晚一点发送出pkt,转发cost就变少了

Suppose each mobile node $N_i \in \mathcal{N}/\{S\}$ has the same cost function $\mathsf{C}(t_i) = b^*(TTL - t_i)$, where $0 \leq t_i \leq TTL$, which represents the cost of forwarding a data packet M from time t_i to the TTL expiration, where b^* is a public cost constant, and t_i is the time at which N_i received the packet. Since node N_i is selfish, the source S should define an incentive policy a^*, and use the payoff $\mathsf{P}(t_i) = a^* \cdot \mathsf{P}_M \cdot \frac{TTL - t_i}{TTL}$ to stimulate N_i to forward M, where $\mathsf{P}(t_i)$ should at least cover the cost $\mathsf{C}(t_i)$, i.e., $\mathsf{P}(t_i) - \mathsf{C}(t_i) \geq 0$. In a strong incentive sense, the utility of N_i should be $\mathsf{U}_i(t_i) = \mathsf{P}(t_i) - \mathsf{C}(t_i) \geq \beta_i \cdot \mathsf{C}(t_i)$, which ensures N_i can get the corresponding $\beta_i \cdot \mathsf{C}(t_i)$ rewards after consuming $\mathsf{C}(t_i)$ costs, where β_i, $0 < \beta_i \leq 1$, is a private selfish factor of N_i and may vary with the current storage, velocity and expected expense of consuming energy of N_i.

Note that mobile relay nodes $\mathcal{N}/\{S\}$ include destinations $SG_j/\{S\}$, as each $N_i \in SG_j/\{S\}$ also expects to increase its gains by forwarding in addition to obtaining the data packet M. Since the source S should pay $\mathsf{P}(t_i)$ for each stimulated node $N_i \in \mathcal{N}/\{S\}$, the actual utility for S thus can be written as $\mathsf{U}_M = \mathsf{P}_M - \sum_{N_i \in \mathcal{N}/\{S\}} \mathsf{P}(t_i) = \mathsf{P}_M \left(1 - \frac{a^*}{TTL} \cdot \sum_{N_i \in \mathcal{N}/\{S\}} (TTL - t_i)\right)$.

S本来准备花掉Pm;然而随time，P(ti)减少，花费减少

C. Security Model

Since our work mainly focuses on stimulating the possible selfish but rational nodes to relay packets while preserving mobile nodes' privacy preservation in OPPNETs, we do not consider the malicious nodes in our security model, i.e., some active attacks like the collusion attack and black/grey hole attacks are currently beyond the scope of this work. Specifically, our security model mainly addresses two security issues: i) how to protect mobile node's privacy in OPPNETs, and ii) how to provide a fair incentive environment in OPPNETs.

D. Design Goal

Our design goal is to develop an efficient incentive and privacy-aware data dissemination scheme in OPPNETs to not only accelerate data dissemination in a fair incentive environment but also protect mobile node's privacy.

III. Proposed IPAD Scheme

In this section, we propose our IPAD scheme, which consists of four phases: system initialization phase, data packet generation phase, data packet dissemination phase, and charging and rewarding phase.

双线性参数//
椭圆 双曲线 加密？

A. System Initialization Phase

For a single-authority OPPNET system under consideration, we assume a trusted authority (TA) is available to boostrap the whole system. Specifically, given the security parameter κ, TA first generates the bilinear parameters $(q, P, \mathbb{G}, \mathbb{G}_T, \hat{e})$ by running $\mathcal{G}en(\kappa)$ [14], where $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a non-degenerated and efficiently computable bilinear map such that $\hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab} \in \mathbb{G}_T$ for all $a, b \in \mathbb{Z}_q^*$ and any $P_1, P_2 \in \mathbb{G}$. TA then chooses a secure symmetric encryption algorithm $\texttt{Enc}()$, e.g., AES, and two collision-resistant cryptographic hash functions H, H_1, where $H : \{0,1\}^* \rightarrow \mathbb{G}$ and $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. In addition, TA also chooses a random number $s \in \mathbb{Z}_q^*$ as the master key, and computes $P_{pub} = sP$. Assume that there are total w virtual social groups $\mathcal{SG} = \{SG_1, SG_2, \cdots, SG_w\}$ in the OPPNET, TA also chooses and maintains a group key K_i for each $SG_i \in \mathcal{SG}$. Finally, TA keeps the master key s secretly, and publishes the system parameter $\texttt{params} = (q, P, \mathbb{G}, \mathbb{G}_T, \hat{e}, H, H_1, \texttt{Enc}(), P_{pub}, \mathcal{SG})$.

Algorithm 1 User Registration

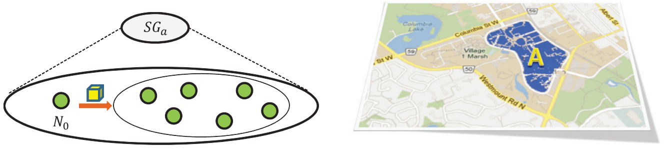
```
procedure UserRegistration
    on input of node $N_i$'s identity and social profile
    TA generates a family of unlinkable pseudo-ID $\mathbb{PID}_i = \{pid_i^{(1)}, pid_i^{(2)}, \cdots, \}$, where each $pid_i^{(j)} \in \mathbb{PID}_i$ is calculated by $pid_i^{(j)} = \texttt{Enc}_s(N_i || r_i^j))$ with random number $r_i^j$ and master key $s$
    For each $pid_i^{(j)} \in \mathbb{PID}_i$, TA computes the corresponding ID-based private key $sk_i^{(j)} \in \mathbb{SK}_i$ where $sk_i^{(j)} = sH(pid_i^{(j)})$
    TA sets $\mathbb{K}_i = \phi$
    for each social group $SG_j \in \mathcal{SG}$ do
        if $U_i$ wants to be a member of $SG_j$ then
            TA assigns the group key $K_j$ to $U_i$, i.e., $\mathbb{K}_i = \mathbb{K}_i \cup \{K_j\}$
        end if
    end for
    return $(\mathbb{PID}_i, \mathbb{SK}_i, \mathbb{K}_i)$
end procedure
```

When a mobile node $N_i \in \mathcal{N}$ registers itself in the system, TA first runs Algorithm 1 to generate all key materials $(\mathbb{PID}_i, \mathbb{SK}_i, \mathbb{K}_i)$ for N_i. In addition, TA maintains a personal credit account (PCA) for N_i, which will be used for N_i's paying and rewarding during the incentive data packet dissemination. Note that, since all pseudo-IDs $pid_i^{(1)}, pid_i^{(2)}, \cdots \in \mathbb{PID}_i$ are unlinkable, N_i can constantly change its pseduo-ID at different location to achieve identity privacy and location privacy in OPPNETs. Meanwhile, since each $pid_i^{(j)} \in \mathbb{PID}_i$ is calculated from $\texttt{Enc}_s(N_i || r_i^j)$, TA can always use the master key s to recover the real identity of node N_i. For the simplicity of description, we use pid_i to represent N_i's any unlinkable pseudo-ID $\in \mathbb{PID}_i$ in the rest of this paper, and its corresponding private key is $sk_i = sH(pid_i)$.

B. Data Packet Generation Phase

Assume node N_0 is a member of social group $SG_a \in \mathcal{SG}$, who wants to send a data packet M to all other members in SG_a, as shown in Fig. 2(a). In particular, N_0 serves as the source S and runs the following steps to generate a packet $\mathcal{P}$.

Step 1: Obtain the current timestamp $\texttt{TS}$, compute the session key $SK_a = H_1(K_a || \texttt{TS})$ with the group key K_a of SG_a, and use SK_a to encrypt M as $C = \texttt{Enc}_{SK_a}(M || \texttt{TS})$.

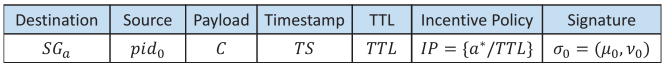


(a) N_0 disseminates a packet in SG_a (b) packet dissemination area $\mathcal{A}$

Fig. 2. N_0 disseminates a data packet to other members in SG_a in area $\mathcal{A}$

Step 2: Set TTL for data packet M and define an appropriate incentive policy $(\texttt{IP})$, which includes an incentive $\frac{a^*}{TTL}$ and can stimulate other mobile nodes $\mathcal{N}/\{N_0\}$ to faithfully store, carry and forward the packet $\mathcal{P}$ if the constraint $\mathsf{U}_i(t_i) = \mathsf{P}(t_i) - \mathsf{C}(t_i) \geq \beta_i \cdot \mathsf{C}(t_i)$ can be satisfied. Note that the detailed incentive policy $(\texttt{IP})$ setting will be discussed in Section IV.

Step 3: Select a random number $r_0 \in \mathbb{Z}_q^*$, compute $\mu_0 = r_0 H(M || \texttt{TS} || TTL || \texttt{IP}) + sk_0$ and $\nu_0 = r_0 P$ to form an ID-based signature $\sigma_0 = (\mu_0, \nu_0)$ [14]. Then, format the packet $\mathcal{P}$ as shown in Fig. 3 for dissemination.



Destination	Source	Payload	Timestamp	TTL	Incentive Policy	Signature
SG_a	pid_0	C	TS	TTL	$IP = \{a^*/TTL\}$	$\sigma_0 = (\mu_0, \nu_0)$

Fig. 3. Packet format in dissemination

C. Data Packet Dissemination Phase

As a member of SG_a, N_0 knows the activities of other SG_a's members are in area $\mathcal{A}$, but does not know their exact locations, as shown in Fig. 2(b). In order to achieve the dissemination efficiency, N_0 will not disseminate the data packet M in the whole area, but only in area $\mathcal{A}$. Suppose that a mobile node N_i comes into N_0's transmission range in area $\mathcal{A}$, N_0 first sends the packet $\mathcal{P}$ to N_i. Then, N_0 and N_i will perform the following contact operations.

- Upon receiving the packet $\mathcal{P}$, N_i first verifies the correctness of the packet and incentive policy $\texttt{IP}$ by checking

$$\hat{e}(\mu_0, P) \overset{?}{=} \hat{e}(\nu_0, H_a)\hat{e}(P_{pub}, H(pid_0)) \tag{2}$$

where $H_a = H(M || \texttt{TS} || TTL || \texttt{IP})$. If it does hold, the packet $\mathcal{P}$ is accepted, and rejected otherwise. The correctness can be verified as follows:

$$\begin{aligned} \hat{e}(\mu_0, P) &= \hat{e}(r_0 H_a + sk_0, P) = \hat{e}(r_0 H_a, P)\hat{e}(sk_0, P) \\ &= \hat{e}(\nu_0, H_a)\hat{e}(P_{pub}, H(pid_0)) \end{aligned} \tag{3}$$

- If N_i is willing to store-carry and forward the packet after checking the incentive policy $\texttt{IP}$ with $\mathsf{U}_i(t_i) = \mathsf{P}(t_i) - \mathsf{C}(t_i) \geq \beta_i \cdot \mathsf{C}(t_i)$, both N_0 and N_i pick up the current timestamp $\texttt{TS}_{0i}$ and make signatures $\sigma_{0*i}, \sigma_{i*0}$ on $\texttt{TS}_{0i} || pid_0 || pid_i || \mathcal{P}$, where

$$\begin{aligned} \sigma_{0*i} &= (\mu_{0*i}, \nu_{0*i}) = (r_{0*i} H_{0i} + sk_0, r_{0*i} P) \\ \sigma_{i*0} &= (\mu_{i*0}, \nu_{i*0}) = (r_{i*0} H_{0i} + sk_i, r_{i*0} P) \end{aligned} \tag{4}$$

with random numbers $r_{0*i}, r_{i*0} \in \mathbb{Z}_q^*$ and $H_{0i} = H(\texttt{TS}_{0i} || pid_0 || pid_i || \mathcal{P})$.

- Then, N_0 and N_i combine σ_{0*i} and σ_{i*0} as σ_{0i}, where

$$\sigma_{0i} = (\mu_{0i}, \nu_{0i}) = (\mu_{0*i} + \mu_{i*0}, \nu_{0*i} + \nu_{i*0}) \quad (5)$$

which allows TA to verify the event that N_0 forwarded the packet $\mathcal{P}$ to N_i at time $\mathtt{TS}_{0i}$ by checking

$$\hat{e}(\mu_{0i}, P) \overset{?}{=} \hat{e}(\nu_{0i}, H_{0i})\hat{e}(P_{pub}, H(pid_0)+H(pid_i)) \quad (6)$$

Note that if N_i is a member of SG_a, it can compute the session key $SK_a = H_1(K_a||\mathtt{TS})$, and use SK_a to recover $M||\mathtt{TS}$ from $C = \mathtt{Enc}_{SK_a}(M||\mathtt{TS})$ individually. If the recovered $\mathtt{TS}$ is corrected, N_i accepts the data packet M at time $\mathtt{TS}_{0i}$ and will pay for the corresponding credit in Eq. (1) to the source in the paying and rewarding phase. Since N_i can individually recover the data packet M, N_0 cannot identify whether N_i is a member of SG_a. As a result, N_i's social profile privacy can be protected in OPPNETs.

Once N_i satisfies the incentive policy ($\mathtt{IP}$), N_i will store-carry and forward the packet $\mathcal{P}$. Specifically, when N_i contacts another mobile node N_j at time $\mathtt{TS}_{ij}$, the Algorithm 2 will be invoked. Obviously, if all mobile nodes satisfy the incentive policy ($\mathtt{IP}$), they all will store-carry and forward the packet $\mathcal{P}$ until the TTL expires. Under such an incentive circumstance, more destinations can quickly receive the data packet M.

Algorithm 2 Incentive Packet Forwarding

```
procedure IncentivePacketForwarding
    When $N_i$, carrying the packet $\mathcal{P}$, contacts $N_j$ at time $\mathtt{TS}_{ij}$
    if $N_j$ does not hold a copy of $\mathcal{P}$ then
        $N_j$ first verifies the packet's correctness by checking Eq. (2)
        if the packet's correctness is verified then
            $N_j$ checks the incentive policy $\mathtt{IP}$
            if $N_j$ satisfies $\mathtt{IP}$ then
                $N_j$ agrees to store, carry and forward the packet $\mathcal{P}$
                $N_i$ and $N_j$ cooperatively generate the signature $\sigma_{ij}$ on $\mathtt{TS}_{ij}||pid_i||pid_j||\mathcal{P}$ by running the similar operations in Eqs. (4)-(5) and keep $\sigma_{ij}$ for the future rewarding
                if $N_j$ is a destination then
                    $N_j$ can generate the session key $SK_a = H_1(\mathtt{TP}||K_a)$ and use it to recover $M$ from $C = \mathtt{Enc}_{SK_a}(M||\mathtt{TS})$
                end if
            end if
        end if
    end if
end procedure
```

D. Paying and Rewarding Phase

In this phase, TA performs the fair credit clearance after the source N_0 submits its incentive policy ($\mathtt{IP}$) and other node $N_j \in \mathcal{N}/\{N_0\}$ reports the time t_j at which N_j received the packet $\mathcal{P}$. Note that the time $t_j = \mathtt{TS}_{ij}$ is extracted from $\mathtt{TS}_{ij}||pid_i||pid_j||\mathcal{P}$, which is authenticated by the signature $\sigma_{ij} = (\mu_{ij}, \nu_{ij})$. Concretely, TA first verifies each signature σ_{ij} by checking $\hat{e}(\mu_{ij}, P) \overset{?}{=} \hat{e}(\nu_{ij}, H_{ij})\hat{e}(P_{pub}, H(pid_i) + H(pid_j))$, where $H_{ij} = H(\mathtt{TS}_{ij}||pid_i||pid_j||\mathcal{P})$, and uses the master key s to identify the real identity N_i from each pseudo-ID $pid_i = \mathtt{Enc}_s(N_i||r_i)$. After that, TA invokes Algorithm 3 to perform paying and rewarding for all mobile nodes $\mathcal{N}$. Since TA is a trusted entity, a fair paying and rewarding can be achieved for all mobile nodes, and node's identity privacy including the source and destionation will not be disclosed to others.

Algorithm 3 Fair Paying and Rewarding

```
procedure FairPayingRewarding
    set $\mathsf{P}_M = 0$
    for each $N_j \in \mathcal{N}/\{N_0\}$ do
        if $N_j \in SG_a/\{N_0\}$ and $N_j$ received the packet at time $t_j$ then
            set $\mathsf{V}(M, t_j) = \begin{cases} \mathbf{v}_m^* \cdot e^{-\mathbf{k}_m(t_j - TTL)}, & \text{if } 0 \le t_j \le TTL \\ 0, & \text{if } t_j > TTL \end{cases}$
            remove $\mathsf{V}(M, t_j)$ from $N_j$'s PCA account
            set $\mathsf{P}_M = \mathsf{P}_M + \mathsf{V}(M, t_j)$
        end if
    end for
    add $\mathsf{P}_M$ to the source $N_0$'s PCA account
    for each $N_j \in \mathcal{N}/\{N_0\}$ and $N_j$ carries the packet since time $t_j$ do
        set $\mathsf{P}_i(t_j) = \begin{cases} \frac{a^*}{TTL} \cdot \mathsf{P}_M \cdot (TTL - t_j), & \text{if } 0 \le t_j \le TTL \\ 0, & \text{if } t_j > TTL \end{cases}$
        transfer $\mathsf{P}_i(t_j)$ from $N_0$'s PCA account to $N_j$'s PCA account
    end for
end procedure
```

IV. Analysis on Incentive Policy

In this section, we analyze the feasibility of our designed Incentive Policy ($\mathtt{IP}$). To abstract the interactions among the mobile nodes $\mathcal{N} = \{N_0, N_1, \cdots, N_{n-1}\}$, we consider a two-party game played by the source N_0 and other nodes $\mathcal{N}/\{N_0\}$. The strategy A_0 available to the source N_0 is that it can choose different incentive factor $\frac{a^*}{TTL}$ on $\mathtt{IP}$ to $\mathcal{N}/\{N_0\}$, while the strategy of each node $N_i \in \mathcal{N}/\{N_0\}$ is to decide whether or not to relay, i.e., the strategy available to N_i includes $A_i = \{\text{Relay}, \neg\text{Relay}\}$. As discussed above, the utility of source N_0 is defined as $\mathsf{U}_M = \mathsf{P}_M \left(1 - \frac{a^*}{TTL} \cdot \sum_{N_i \in \mathcal{N}/\{N_0\}} (TTL - t_i)\right)$ when each $N_i \in \mathcal{N}/\{N_0\}$ decides to relay, and a low value when some nodes decide not to relay. The utility of each node $N_i \in \mathcal{N}/\{N_0\}$ is $\mathsf{U}_i(t_i) = \mathsf{P}(t_i) - \mathsf{C}(t_i)$ when it decides to relay packet and $\mathsf{U}_i(t_i) = 0$ otherwise. Each N_i is rational to maximize its utility, and it will decide to relay only when $\mathsf{P}(t_i) - \mathsf{C}(t_i) \ge \beta_i \cdot \mathsf{C}(t_i)$, where $0 < \beta_i \le 1$ is a private selfish factor and unavailable to the source. Therefore, the two-party game is a game with imperfect information. For the source N_0, the more the nodes serve as relays, the higher utility it can gain. Therefore, in order to stimulate all nodes $\mathcal{N}/\{N_0\}$, the source should provide a proper incentive $\frac{a^*}{TTL}$. On the other hand, for any node $N_i \in \mathcal{N}/\{N_0\}$, the constraint $\mathsf{P}(t_i) - \mathsf{C}(t_i) \ge \beta_i \cdot \mathsf{C}(t_i)$ can be written as

$$\frac{a^*}{TTL} \cdot \mathsf{P}_M \cdot (TTL - t_i) \ge (1 + \beta_i) b^* (TTL - t_i) \quad (7)$$

that is, $\frac{a^*}{b^* \cdot TTL} \ge \frac{(1+\beta_i)}{\mathsf{P}_M}$. To guarantee node N_i can always be stimulated, the constraint should still hold when P_M is minimal, i.e., $\frac{a^*}{b^* \cdot TTL} \ge \frac{1+\beta_i}{\min(\mathsf{P}_M)}$.

In the following, we estimate the average value of $\min(\mathsf{P}_M)$ in our considered OPPNET. Assume that there are total η destinations $SG_a/\{N_0\}$. If all η destinations receive the packet $\mathcal{P}$ later than other nodes $\mathcal{N}/SG_a$, as shown in Fig. 4, $\mathsf{P}_M = \mathbf{v}_m \cdot \sum_{N_i \in SG_a/\{N_0\}} e^{-\mathbf{k}_m(t_i - TTL)}$ will reach its min-

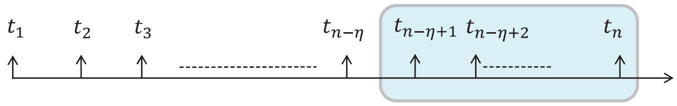


Fig. 4. η destinations received the packet $\mathcal{P}$ later than other nodes

imal value. Since all pairwise contacts follow a homogenous Possion process with contact rate λ in our network model, if k nodes have already carried copies of packet $\mathcal{P}$, the probability that one node in the rest $(n-k)$ nodes can receive a copy within time t can be obtained by $\Pr\{T < t\} = 1 - e^{-\lambda k(n-k)t}$, and the average delay is achieved by $\bar{t}_{k+1} = \frac{1}{\lambda k(n-k)}$. Therefore, the average delay that the $(k+1)$-th copy is generated can be written as $t_{k+1} = \sum_{i=1}^{k} \frac{1}{\lambda i(n-i)}$. Then, the time $(t_{n-\eta+1}, t_{n-\eta+2}, \cdots, t_n)$ for η destinations received the packet $\mathcal{P}$ can be determined, i.e.,

$$t_{n-\eta+i} = \begin{cases} \frac{1}{\lambda n}(\mathsf{H}_{n-\eta+i} + \mathsf{H}_{n-1} - \mathsf{H}_{\eta-i-1}), \\ \qquad\qquad \text{for } 1 \leq i \leq \eta - 1; \\ \frac{2}{\lambda n}\mathsf{H}_{n-1}, \qquad \text{for } i = \eta. \end{cases} \tag{8}$$

where H_{n-1} is the $(n-1)$-th harmonic number. Then, put $(t_{n-\eta+1}, t_{n-\eta+2}, \cdots, t_n)$ into $\mathsf{P}_M = \mathbf{v}_m \cdot \sum_{N_i \in SG_a/\{N_0\}} e^{-\mathbf{k}_m(t_i - TTL)}$, the minimal value of P_M can be derived. Since b^* is a constant for all mobile nodes and TTL is set by the source, the source can determine the incentive factor $\frac{a^*}{TTL} \geq b^* \cdot \frac{1+\beta_i}{\min\{\mathsf{P}_M\}}$. Therefore, we have the following Lemma.

Lemma 1: To achieve an effective incentive, the best strategy for the source is to set the incentive factor $\frac{a^*}{TTL} = \frac{2b^*}{\min\{\mathsf{P}_M\}}$ in $\mathtt{IP}$.

Proof. Let the source choose a small incentive $a^{*-} < a^*$. Since each node N_i's private selfish factor β_i is unknown, there may exist some β_j such that $\frac{a^{*-}}{b^* \cdot TTL} < \frac{1+\beta_i}{\min\{\mathsf{P}_M\}}$ for node N_j. Then, since N_j is not fully stimulated, N_j will deny participating in the nodal cooperation, and destinations will take a long time to receive the packet, which will reduce the value of P_M, and subsequently decrease the source's utility U_M. Since $2 \geq 1 + \beta_i$, we have $\frac{a^*}{TTL} = \frac{2b^*}{\min\{\mathsf{P}_M\}} \geq \frac{(1+\beta_i)b^*}{\min\{\mathsf{P}_M\}}$. Then, $\frac{a^*}{TTL} = \frac{2b^*}{\min\{\mathsf{P}_M\}}$ can fully stimulate all mobile nodes $\mathcal{N}/\{N_0\}$. On the other hand, if the source chooses a large incentive $a^{*+} > a^*$, the value of P_M will not increase because $\mathcal{N}/\{N_0\}$ have already been full stimulated, yet the source has to pay more $\frac{a^{*+}}{TTL} \cdot \mathsf{P}_M \cdot \sum_{N_i \in \mathcal{N}/\{N_0\}} (TTL - t_i)$ to $\mathcal{N}/\{N_0\}$. As a result, the best strategy for the source is to set $\frac{a^*}{TTL} = \frac{2b^*}{\min\{\mathsf{P}_M\}}$ in $\mathtt{IP}$. ■

With the incentive factor $\frac{a^*}{TTL} = \frac{2b^*}{\min\{\mathsf{P}_M\}}$, we also can use the following lemmas to show the best strategy for each mobile node in $N_i \in \mathcal{N}/\{N_0\}$ is "Relay", i.e., faithfully store, carry and forward the packet $\mathcal{P}$ for maximizing its utility in OPPNETs, as shown in Fig. 5.

Lemma 2: When N_i contacts N_j, the best strategy of N_j is to store the packet $\mathcal{P}$ if it has not carried the packet. ■

Lemma 3: When N_i contacts N_j, the best strategy of N_i is to forward the packet $\mathcal{P}$ to N_j immediately. ■

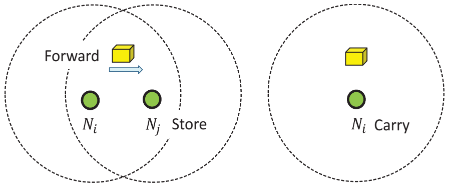


Fig. 5. "Store-Carry-Forward" is the best strategy of each $N_i \in \mathcal{N}/\{N_0\}$

Lemma 4: When N_i does not contact N_j and its own storage requirement is not intense, the best strategy of N_i is to carry the packet until the TTL expires. ■

Summarizing the above Lemmas, we can see that, once the source provides a secure incentive $\frac{a^*}{TTL} = \frac{2b^*}{\min\{\mathsf{P}_M\}}$, other mobile nodes are willing to participate in nodal cooperation for data dissemination in the OPPNET.

V. Conclusions

In this paper, we have proposed a credit-based incentive and privacy-aware data dissemination (IPAD) scheme for OPPNETs, which mainly exploits how to simultaneously protect mobile node's privacy and provide a fair incentive for efficiently disseminating a time-valuable data in privacy-aware OPPNETs. In our future work, we will exploit a privacy-aware OPPNET with co-existing selfish and malicious nodes, and develop secure mechanisms to not only stimulate selfish nodes but also identify malicious nodes in the challenging scenario.

References

[1] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 134 – 141, 2006.

[2] R. Lu, X. Lin, T. H. Luan, X. Liang, X. Li, L. Chen, and X. Shen, "Prefilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks," in *INFOCOM*, 2012, pp. 1395–1403.

[3] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *INFOCOM*, 2010, pp. 632–640.

[4] ——, "Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, to appear.

[5] C. Boldrini, M. Conti, and A. Passarella, "Context and resource awareness in opportunistic network data dissemination," in *WOWMOM*, 2008.

[6] T.-K. Huang, C.-K. Lee, and L.-J. Chen, "Prophet+: An adaptive prophet-based routing protocol for opportunistic network," in *AINA*, 2010, pp. 112–119.

[7] G. Bigwood and T. Henderson, "Bootstrapping opportunistic networks using social roles," in *WOWMOM*, 2011, pp. 1–6.

[8] R. Lu, X. Lin, H. Zhu, X. Shen, and B. R. Preiss, "Pi: a practical incentive protocol for delay tolerant networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1483–1493, 2010.

[9] L. Lilien, Z. Kamal, V. Bhuse, and A. Gupta, "The concept of opportunistic networks and their research challenges in privacy and security," *Mobile and Wireless Network Security and Privacy In Mobile and Wireless Network Security and Privacy*, pp. 85–117, 2007.

[10] I. Parris and T. Henderson, "Privacy-enhanced social-network routing," *Computer Communications*, vol. 35, no. 1, pp. 62–74, 2012.

[11] Z. Le, G. Vakde, and M. Wright, "Peon: privacy-enhanced opportunistic networks with applications in assistive environments," in *PETRA*, 2009.

[12] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[13] R. Groenevelt, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," *Perform. Eval.*, vol. 62, no. 1-4, pp. 210–228, 2005.

[14] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in *Public Key Cryptography*, 2006, pp. 257–273.